



# UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/756,346	01/08/2001	Henry Haverinen	442-010085-US (PAR)	6669
2512	7590	11/25/2005	EXAMINER	
PERMAN & GREEN 425 POST ROAD FAIRFIELD, CT 06824			SIMITOSKI, MICHAEL J	
			ART UNIT	PAPER NUMBER
			2134	
DATE MAILED: 11/25/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)	
	09/756,346	HAVERINEN ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 30 September 2005.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-13, 15, 17-20 and 22-30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-10, 12, 13, 15, 17-20, 22, 23 and 25-30 is/are rejected.
- 7) ☒ Claim(s) 11 and 24 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 March 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |   |   |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                                    |

### **DETAILED ACTION**

1. The response of 9/30/2005 was received and considered.
2. Claims 1-13, 15, 17-20 & 22-30 are pending.
3. Claims 11 & 24 are objected to.

### ***Response to Arguments***

4. In light of Applicant's amendment to claim 24, the rejection of that claim under 35 U.S.C. §112 is withdrawn.
5. Applicant's arguments filed 9/30/2005 have been fully considered but they are not persuasive.
6. Applicant's response (p. 16, ¶4) argues that the combination of Federrath, Sayers and Menezes lacks providing the packet data network with authentication information usable by the telecommunications network. It is noted that this limitation is not recited in claims 13, 15, 17-19, 20 and 22-27. However, Federrath discloses authenticating one network to another (Fig. 1), but lacks the second network being specifically a packet data network (Federrath discloses GSM, which is in fact a packet data network, however in light of Applicant's specification, the Sayers reference is included to teach a non-mobile phone network). Sayers teaches that mobile phones using GSM can access other networks, such as LANs (col. 6, lines 58-65), which importantly to the present invention can support call connection in the wired protocol (col. 10, lines 49-62). Therefore, one of ordinary skill would have been motivated to perform the authentication of Federrath regarding the visited network in the "packet data network" of Sayers. As modified even by Sayers, however, Federrath lacks providing the mobile node with a protection code, sending the protection code with the mobile node identity/TMSI, forming cryptographic

Art Unit: 2134

information using at least the protection code and the session secret, sending the cryptographic information with the challenge to the mobile node/station and checking at the mobile node the validity of the cryptographic information using the challenge and the shared secret. However, this is a well-known concept in cryptography where a random number is used in challenge-response protocols to provide timeliness assurances and avoid replay attacks (§10.3.1). This is accomplished where a receiving party (network) creates a response (cryptographic information) that depends on a secret/ $K_c$  and the challenge/nonce (protection code (§10.3 & §10.3.1). Further it is noted that the authentication information being “usable by the telecommunications network” is not limiting, in that the claim does not recite the characteristics of what makes the information “usable” nor does the claim recite for what the information is usable. As both networks in Federrath and Sayers receive, transmit and process data, the authentication information is usable by each network.

7. Applicant's response (p. 17, ¶4) argues that all that Sayers may add [to Federrath] is that “GSM can be used as a radio access mechanism and to access further private networks.”

However, Sayers teaches that a mobile access network (such as GSM) can be used as a network to access a second network, such as a private LAN. Therefore, in combination, the Sayers GSM network is similar to the home network of Federrath, but as modified, Federrath's mobile node (Federrath, Fig. 1) can authenticate to a private network (Sayers, col. 6, lines 58-65). An example when this authentication would be beneficial is given in Sayers where the mobile node uses a private network to establish call connection in a standard wired protocol (col. 10, lines 49-62). Applicant's response (p. 17, ¶4 – p. 18, ¶1) argues further that Sayers discloses one GSM network interoperating with the others so only that this network employs IP in data exchange

Art Unit: 2134

between its network elements. The Examiner notes that IP is not recited in the claims, nor is the protocols through which the packet data and telecommunications networks utilize. Further, applicant notes that the air interface in Sayers is that of GSM. The Examiner notes that the claims make no recitation of which of the networks, if any, in the claim utilize an air interface.

8. Applicant's response (p. 18, ¶2-3) argues that the invention "relates to authenticating a terminal to a packet data network" and further that the Sayers network "is not seen by the terminal as a packet data network if the terminal communicates with it only using circuit switched data known from GSM." In response, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. Further, it is noted that this limitation is not recited in claims 15, 17-19 & 23-27. The Examiner notes that the claims make no recitation that the terminal communicate in any particular protocol, simply that data is sent and is usable. In response, as described above, Federrath discloses authenticating between two networks to authenticate a mobile node. Sayers discloses that one network in a communication with a mobile node can be a packet data network. In combination, the Federrath mobile node can authenticate to the private network of Sayers, rather than the home network of Federrath. This combination is obvious because Sayers teaches that a mobile node can establish a call connection with the wired, private network (col. 10, lines 49-62), and the Federrath reference is disclosing making a call connection (Fig. 1). Further, Applicant suggests that Sayers does not disclose or suggest an actual telecommunications network. However, Applicant is directed to col. 10, lines 49-62 where Sayers discusses making a call connection.

9. Applicant's response (p. 19, last ¶) argues that "Sayers and Federrath already make use of the Fundamentals of cryptography discussed by the Handbook of Applied Cryptography written by Menezes and that there is no motivation to private "a new extra security mechanism on top of GSM". While Menezes teaches that performing authentication in a secure manner is beneficial, and therefore provides proper motivation, Applicant's assertion appears to be claiming that any improvement or additional security protocol steps above what is already disclosed in GSM would be unobvious, simply because GSM already contains security. The Examiner respectfully disagrees.

10. Applicant's response (p. 20, ¶2) argues that "the basics of cryptography are understood by the developers of GSM". However, the Examiner respectfully asserts that the claim must be examined from the point of view of one of ordinary skill in the art, and it is not within the purview of the Examiner to speculate as to what was "understood" by the "developers of GSM." Certainly, however, no assertion can be made that any changes or improvements to GSM are unobvious or impossible simply because the developers of the protocol understand cryptography. Again, because Federrath is concerned with authentication to set up a call and Sayers presents a method of setting up a call with respect to a wired protocol, the combination to use the protocol of Federrath to communicate with a private network is proper.

11. Applicant's response (§5) argues that Brown discloses only the use of a SIM card for authentication in different telecom systems and using a challenge and response. However, Brown is cited for teaching specific details of the SIM card, as taught by Federrath, where Brown further teaches that the SIM card is programmed with the subscriber identity and shared secret, which is used to calculate the session secret (col. 5, line 26 – col. 6, line 3).

12. Applicant's response (§7) argues that “Abrol does not disclose or suggest that improvements for an existing authentication system would be used as described in Applicant’s invention.” In response, Applicant is referred to the previous Office Action for the application of Abrol regarding the claims. Applicant's arguments regarding specifically the Abrol reference fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

13. For the above reasons, the rejections are maintained. However, Applicant is reminded that claims 11 & 24 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The Examiner’s reason for indicating allowable subject matter is given below.

***Claim Rejections - 35 USC § 103***

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

15. Claims 1, 3-5, 8-10, 13, 19, 20, 22 & 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over “Protection in Mobile Communications” by **Federrath**, in view of U.S. Patent 6,539,237 to Sayers et al. (**Sayers**) in view of Handbook of Applied Cryptography by Menezes et al. (**Menezes**).

Regarding claims 1, 3-4, 9-10, 13, 19, 20, 22 & 28-30, Federrath discloses providing the mobile node/station with a mobile node identity/TMSI and a shared secret/Ki specific to the mobile node identity/TMSI and usable by a telecommunications network/home network (Fig. 1, p. 5), sending the mobile node identity/TMSI from the mobile node to the network/visited network, providing the network/visited network with authentication information usable by the telecommunications network/home network, the authentication information comprising a challenge/RAND and a session secret/Kc corresponding to the mobile node identity/TMSI and derivable using the challenge/RAND and the shared secret/Kc (Fig. 1, p. 5), sending the challenge/RAND from the network/visited network to the mobile node/station (Fig. 1, p. 5), generating at the mobile node the session secret/Kc and a first response corresponding/SRES to the challenge/RAND, based on the shared secret/Ki (Fig. 1, p. 5), sending the first response/SRES to the packet data network, and checking/authenticating the first response for authenticating the mobile node (Fig. 1, p. 5). Federrath lacks the visiting network being specifically a packet data network. However, Sayers teaches that as wireless technology becomes more popular, companies desire to let workers increase mobility and access all voice and data information via wireless networks (col. 6, lines 58-65). Sayer's system comprises a private wireless network (Fig. 2) where mobile stations/phones communicate with protocol converters (P-BTS) that communicate with an IP network, such as the Internet (Fig. 2, #24) through a protocol interface (Fig. 2, #28-1) (see also col. 9, lines 26-65). Further, Sayers teaches that the software of the P-BTSs provide support for call connection in the wired protocol (col. 10, lines 49-62). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Federrath to allow the mobile units to interact with a



wired network, such as an IP network. One of ordinary skill in the art would have been motivated to perform such a modification to allow users to access all voice and data information via wireless networks, as taught by Sayers (Fig. 2, col. 6, lines 58-65, col. 9, lines 26-65 & col. 10, lines 49-62). As modified, Federrath lacks providing the mobile node with a protection code, sending the protection code with the mobile node identity/TMSI, forming cryptographic information using at least the protection code and the session secret, sending the cryptographic information with the challenge to the mobile node/station and checking at the mobile node the validity of the cryptographic information using the challenge and the shared secret. However, Menezes teaches that random numbers can be used in challenge-response mechanisms to provide timeliness assurances and avoid certain replay and interleaving attacks (§10.3.1 (i)). Menezes teaches that nonces can be used to provide timeliness guarantees where a receiving party (network) creates a response (cryptographic information) that depends both on a secret/ $K_c$  and the challenge/nonce (protection code) (§10.3 & §10.3.1 Background). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide the mobile node with a protection code/nonce, send the protection code/nonce with the mobile node identity/TMSI, form cryptographic information/nonce verification using at least the protection code/nonce and the session secret/ $K_c$ , send the cryptographic information/nonce verification with the challenge/RAND to the mobile node/station and check at the mobile node the validity of the cryptographic information/nonce verification using the challenge/RAND and the shared secret/ $K_i$ . One of ordinary skill in the art would have been motivated to perform such a modification to distinguish one protocol instance from another and to prevent certain chosen-text attacks in challenge-response protocols, as taught by Menezes (§10.3 & §10.3.1).

Regarding claim 5, Federrath, as modified above, discloses a link not being a link of the telecommunications network (visited network) (p. 5, Fig. 1).

Regarding claim 8, Federrath discloses obtaining a second response/SRES' by the telecommunications network/home network, and using the second response in the checking/(auth.result =?) the first response (p. 5, Fig. 1).

16. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Federrath** in view of **Sayers** and **Menezes**, as applied to claim 1 above, in further view of "The Network Access Identifier" by Aboba et al. (**Aboba**). Federrath, as modified above, lacks forming a Network Access Identifier from the subscriber identity/TMSI as the mobile node identity. However, Aboba teaches that the network access identifier is known in the art as an identifier for a user, to be used in roaming and to assist in routing an authentication request (§2.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to form a network access identifier as the mobile node identity by the mobile node, from the subscriber identity. One of ordinary skill in the art would have been motivated to perform such a modification to assist in routing an authentication request, as taught by Aboba (p. §2.1).

17. Claims 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Federrath** in view of **Sayers** and **Menezes**, as applied to claim 1 above, in further view of U.S. Patent 5,537,474 to Brown et al. (**Brown**). Federrath, as modified above, discloses using a Subscriber Identity Module, but lacks using it for the providing the mobile node with the mobile node identity and generating the session secret. However, Brown teaches that the mobile device in the

Art Unit: 2134

GSM system includes a SIM, programmed with the subscriber identity and shared secret/ $K_i$ , which calculates the session secret/ $K_c$  (col. 5, line 26 – col. 6, line 3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the SIM for the providing the mobile node with the mobile node identity and generating the session secret. One of ordinary skill in the art would have been motivated to perform such a modification to conform to the GSM standard, as is well known in the art, and taught by Brown (col. 5, line 39 – col. 6, line 3).

18. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Federrath** in view of **Sayers** and **Menezes**, as applied to claim 1 above, in further view of “Internet Key Exchange (IKE)” by Harkins et al. (**Harkins**) in further view of Applied Cryptography, Second Edition by **Schneier**. Federrath, as modified above, lacks generating a session key for Internet Key Exchange, wherein the shared session key is based on the at least one session secret and the at least one challenge. However, Harkins teaches that Internet Key Exchange is a protocol used to establish authenticated keying material in IPSec (§1 & §2), which is authenticated using a pre-shared key (§5.4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a session key for Internet Key Exchange. One of ordinary skill in the art would have been motivated to perform such a modification to use IPSec, as taught by Harkins (§1-2 & §5.4). As modified, Federrath lacks the session key being based on the session secret and at the challenge. However, Schneier teaches that a ‘salt’ is a random string applied to a password to make it more difficult to find using a dictionary attack. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was

made to 'salt' the session secret/password with the challenge/random string. One of ordinary skill in the art would have been motivated to perform such a modification to make the session secret more difficult to find using a dictionary attack, as taught by Schneier (pp. 52-53).

19. Claims 15, 17, 18 & 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Federrath** in view of **Sayers, Menezes** and WO 01/41470 to **Abrol et al. (Abrol)**.

Regarding claims 15, 17, 18 & 26-27, the claims are substantially equivalent to claim 1, but lack a gateway/network entity acting as an interface. However, Abrol teaches that by using a data service node/gateway that supports authentication between a mobile node and an authentication server, the benefit of providing authentication for a diverse set of mobile stations in a wireless network is gained (p. 3, ¶2-3). The data service node/gateway performs authentication techniques for the mobile station; otherwise, an authentication server is accessed (p. 3, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an authentication gateway/data service node to authenticate mobile stations. One of ordinary skill in the art would have been motivated to perform such a modification to provide authentication for a diverse set of mobile stations in a wireless network, as taught by Abrol (p. 3, ¶2-3).

Regarding claim 27, Federrath discloses the mobile node being integrated with a mobile station (Fig. 1) and a terminal part providing the subscriber identity and shared secret to the mobile node and mobile station

Art Unit: 2134

20. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Federrath** in view of **Sayers, Menezes and Abrol**, as applied to claim 15 above, in further view of **Aboba**. Federrath, as modified above, lacks forming a Network Access Identifier from the subscriber identity/TMSI as the mobile node identity. However, Aboba teaches that the network access identifier is known in the art as an identifier for a user, to be used in roaming and to assist in routing an authentication request (§2.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to form a network access identifier as the mobile node identity by the mobile node, from the subscriber identity. One of ordinary skill in the art would have been motivated to perform such a modification to assist in routing an authentication request, as taught by Aboba (p. §2.1).

21. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Federrath** in view of **Sayers, Menezes and Abrol**, as applied to claim 15 above, in view of **Harkins and Schneier**. Federrath, as modified above, lacks generating a session key for Internet Key Exchange, wherein the shared session key is based on the at least one session secret and the at least one challenge. However, Harkins teaches that Internet Key Exchange is a protocol used to establish authenticated keying material in IPsec (§1 & §2), which is authenticated using a pre-shared key (§5.4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a session key for Internet Key Exchange. One of ordinary skill in the art would have been motivated to perform such a modification to use IPsec, as taught by Harkins (§1-2 & §5.4). As modified, Federrath lacks the session key being based on the session secret and at the challenge. However, Schneier teaches that a 'salt' is a random string

Art Unit: 2134

applied to a password to make it more difficult to find using a dictionary attack. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to 'salt' the session secret/password with the challenge/random string. One of ordinary skill in the art would have been motivated to perform such a modification to make the session secret more difficult to find using a dictionary attack, as taught by Schneier (pp. 52-53).

### *Allowable Subject Matter*

22. The following is a statement of reasons for the indication of allowable subject matter:

Regarding claim 11, the prior art relied upon fails to teach or suggest the challenge being based on RAND codes of at least two authentication triplets of the telecommunications network, in combination with the other elements of the claim.

Regarding claim 24, the prior art relied upon fails to teach or suggest receiving at least two challenges corresponding to the mobile node identity from the authentication server, forming cryptographic information based on the at least two received challenges and to output the two received challenges and the cryptographic information for transmission to the mobile node, in combination with the other elements of the claim.

### *Conclusion*

23. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2134

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

**Any response to this action should be mailed to:**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**Or faxed to:**

(571) 273-8300  
(for formal communications intended for entry)

**Or:**

(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

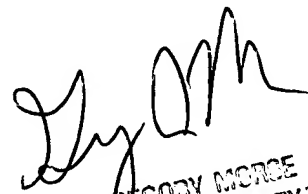
Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



MJS

November 14, 2005



GREGORY MORCE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2.00